OTOP’s Information Technology Policy Program

Framework for EPA’s IT Policies

Version 1.0

March 2003

Introduction and Purpose

This document will provide OEI/OTOP management with recommendations to address information technology (IT) policy vulnerabilities. The recommendations are based on Federal Information Resources Management (IRM) legislation and guidance and the OEI organizational structure that was established to “fundamentally realign information management and policy at EPA.” The ultimate goal is to bring EPA’s IT policy into compliance with IRM-related Federal legislation; guidance from the Office of Management and Budget (OMB), General Accounting Office (GAO), and National Institute of Standards and Technology (NIST); industry and government best practices; and the current state of information technology. A viable EPA IT policy program will help ensure that information and information technology are managed as strategic resources to help meet the Agency’s mission.

The development of this IT policy program and the delineation of IT policy requirements will also address issues identified in the 2002 Audit Report of the Office of Inspector General (OIG): “Information Technology: EPA Management of Information Technology Resources Under the Clinger-Cohen Act.” In the report, the IG stated that the CIO should provide “technical IRM expertise and establish management policies and procedures that will provide a control framework to integrate EPA’s information technology environment and core business processes.”

This document defines the framework to be used to organize the substantive content of OTOP IT policy documents. It is intended to be used in conjunction with OTOP's previously established Standard Operating Procedure for IT Policy Development which defines the functional tiering structure for IT policies: Tier 1 -- Policies, Tier 2 -- Procedures, Tier 3 -- Technical Operations and Standards (TOPS), and Tier 4 -- Guidelines. Any of the policy categories in this framework may have documents developed in any or all of the 4 Tiers.

It is vitally important to note that all of EPA’s IRM requirements should be considered while developing an IT policy program. EPA’s IT policy requirements, by necessity, have inter-relationships with the information management policies of the other OEI organizations. In the interest of consistency and cohesiveness, these inter-relationships must be considered in the development of OTOP’s IT Policy Framework. However, it is not in the scope of this document to identify the policy requirements of other OEI offices. This document is the Framework for EPA's IT policies.

Intended Audience

This document is for the OEI/OTOP managers to help identify and define IT policy categories. It is the first step in determining the current status and vulnerabilities of EPA's IRM/IT policy program.

IRM/IT Legislation, Regulations, and Guidance

The following list of laws, regulations, and executive guidance is not an exhaustive list. However it identifies the MAJOR sources of requirements for a Federal IT policy program:

- Chief Financial Officers Act of 1990 (CFO)
- Clinger-Cohen Act of 1996 (CCA)
- Computer Security Act of 1987 (CSA)
- E-Government Act of 2002 (see also FISMA)
- The Federal Acquisition Reform Act of 1995
- The Federal Acquisition Streamlining Act (FASA) of 1994
- Federal Information Security Management Act of 2002 (FISMA)
- Government Paperwork Elimination Act of 1999 (GPEA)
- Government Performance and Results Act of 1996 (GPRA)
- Homeland Security Act of 2002
- Paperwork Reduction Act of 1995 (PRA)
- Public Law 107-217, Title 40 USC, Public Buildings, Property, and Works, Subtitle III, Information Technology Management
- Executive Order 13011, Federal Information Technology
- OMB Memorandum M-96-20, "Implementation of the Information Technology Management Reform Act of 1996" (known as the Clinger-Cohen Act of 1996)
- OMB Circular A-11, Part 3, "Planning Budgeting and Acquisition of Capital Assets."
- OMB Circular A-130, "Management of Federal Information Resources"
- Presidential Decision Directives (PDD) 63, Critical Infrastructure Protection, 1998
- Presidential Memorandum, Implementing Government Reform, July 11, 2001

Categories (Elements/ Tracks/Segments)

The following five IT policy categories cover the breadth of IT functional areas needed to comply with Federal requirements/IT activities and form a complete IT policy program. The subjects within each of the five categories cover the issues identified to date. Additional subjects may be added to the framework in the future as they are identified.

I. IT Planning and Acquisition

   A. Financial
      - Working Capital Fund
      - Budgeting
   B. Strategic Planning
   C. Systems Life Cycle Management
   D. IT Investment Management
   E. Hardware Acquisition
   F. Software Acquisition/Development

II. Enterprise Architecture and Standards

   A. IT Architecture
   B. Accessibility
   C. Integration
   D. E-Government

III. IT Operations

   A. Hardware; for example:
      - Mainframes
      - Supercomputer
      - Desktop, laptops, and other PCs
      - Servers, routers and switches
      - Equipment
         - Phones
         - FAX
         - Wireless
         - Personal Digital Assistants (PDAs)
   B. Software, including
      - Installation
      - Post-implementation Review(s)
      - Management
   C. Facilities, for example:
      - Washington Information Center (WIC)
      - Systems Development Center (SDC)
      - National Computer Center (NCC)
      - Technical Support Center (TSC)
      - Local Computer rooms
   D. Telecommunications, for example:
      - Network, such as
         - LANs
         - WAN
         - Internet and Intranet
         - Extranet

IV. IT Security

The security policy area is a cross-cutting category and may be incorporated into or cross-referenced with the other categories as appropriate.

A. Risk Assessments
B. Security Plans
C. FISMA of 2002
D. PDD - 63
E. COOP

V. Administrative and Business Policies for IT

A. Human Resources Capital
B. Staffing, for example:
   - Retention issues
   - Knowledge management
   - Quantity of staff
   - Personnel security, i.e., background checks
   - IT skills requirements - Workforce assessment
C. Training, for example:
   - IT staff's technical skills
   - End users for policy awareness and understanding
   - Program specific
   - Executive and manager training
   - Security training/awareness
D. Topic Specific, for example:
   - Limited Personal Use of Government Office Equipment
   - Customer Relations Strategy

It is important to note that not all material and subjects contained in the current EPA IRM Policy Manual 2100 and in other stand-alone IT policy documents are considered top-level (Tier 1) policy. Procedures, technical operational directives and standards, and guidance dominate much of the current documentation. These are components of OEI's Policy Tiers 2 - 4. Policy tiering requirements must be considered when developing EPA's IT policy and supporting documentation.

Definitions of Categories

The following definitions describe the policy categories. However, the issues and topics within each category are not limited to those described below. Other topics or issues can be added within the categories as policy requirements are identified.

I. IT Planning and Acquisition

This category includes policies applicable to the technology acquisition and investment control requirements of the Clinger Cohen Act of 1996 (CCA). Policies in this category will help integrate and/or link business processes and IT tools, while promoting cost benefits and controls. It sets the requirements for the formulation of system development and implementation plans, such as those found in the System Life Cycle Management Policy.

IT financial management requirements relate to the budget process and include all policies and guidelines concerning the financial aspects of the Working Capital Fund (WCF) and IT Investment Management.

II. Enterprise Architecture and Standards

The Enterprise Architecture program and policies will provide the foundation of the Agency's technology requirements to meet Agency business needs. It will also include and set standards to facilitate integrating data across programs. Integration is a major requirement in the newly enacted Federal E-Government Act of 2002.

III. IT Operations

Operational policies will identify and describe the operating efficiency and capacity of EPA's IT hardware, software, and facility operations, and telecommunications. It will describe the day-to-day system management responsibility for EPA's IT infrastructure. This includes but is not limited to

- Computer operational activities (mainframes - including supercomputer, LAN, WAN, Servers, PCs, etc.)
- Power equipment
- Physical facilities (e.g., WIC, NCC, TSC, and SDC)

This category will include principles that govern the electronic transfer of information (voice and data) between and among Agency sites and organizational components, as well as between the Agency and the customers we serve.

IV. IT Security

EPA policy on IT security is relatively current. However, the basic policies are mixed with guidelines and procedures. The Security program will need to reflect the proposed format of OEI's Policy Tiers. Security is also a component of the other policy categories and may be cross-referenced from this category.

V. Administrative Business Policies for IT

IT training is not sufficiently addressed in most current IT policies. A recent exception (in Spring 2002) is the information technology planning and acquisition training (a significant element and requirement of the CCA) which is being incorporated into the Agency's IT Investment Management program and process. EPA's IT training program for updating and increasing IT staff skills, end-user training, and other requirements such as security training and Policy Awareness training, may require new, or editing current, policies to document training requirements. Other areas, such as customer service and performance measurement may be incorporated into particular policies and supporting documents. Other IT administrative polices may include IT human resources needs and requirements, and employee-related policies such as Limited Personal Use of Government Office Equipment, and customer service policies.